PKI Usage

PKI is an enabler, supporting changing processes to more efficiently conduct daily business. The most common uses of PKI are digitally signing and encrypting email. However, the most significant advantage is derived from PK-enabling software applications. This advantage allows the Army and its supporting organizations to realize substantial benefits by implementing electronic-based PKI processes. These benefits include cost savings and/or quality and performance improvements which cannot be realized without re-engineering current business processes. The lists below represent only a small portion of potential applications.

Current PKI usages:

- Sending and receiving digitally signed emails
- Sending and receiving encrypted emails
- Logging on to computes/networks

Current PKE pilots:

- Defense Travel System (DTS)
- Defense Finance and Accounting Systems (DFAS)
- Corps of Engineers Financial Management System

PKI is a cost-effective technology allowing organizations to re-engineer and streamline business practices while protecting vital information. PKI will become a ubiquitous part of how data is sent/received and daily Army business conducted.

For Assistance Contact:

IA CAC/PKI Help Desk

Hours of Operations: 0730-1630 Eastern Time Zone

Phone: 703-769-4499
DSN: 327-4004
Toll Free: 1-866-738-3222
Fax: 703-769-7605
Email: iacacpki.helpdesk@us.army.mil

See the **IA CAC/PKI** web site for:

- Help information
- Frequently Asked Questions (FAQs)
- Troubleshooting
- Training Information

Understanding Public Key Infrastructure

September 2005

Submitted by
Army Information Assurance
CAC/PKI Training
2110 Washington Boulevard, Suite 200
Arlington VA 22204

« *Teach me what I need to know to do my job…* »

Public Key Infrastructure – PKI

Throughout modern history, there has been a need for information assurance—for confidentiality, authentication, verification, contract validation, and data integrity. Cryptography and other forms of security services were developed to meet those needs. PKI uses cryptographic technology that has existed for more than twenty years, but has recently gained recognition as a scalable solution for Information Assurance (IA) across the Enterprise.

The Secretary of Defense has mandated PKI deployment throughout the Department. DoD PKI is predicted on providing Information Assurance supporting a broad range of applications. As more business is conducted digitally, PKI increases the assurance that electronic transactions are secure.

PKI Security Services

PKI provides a foundation for interoperable, Public Key Enabled (PKE) security services at multiple assurance levels for the warfighter's business process improvements.

PKI provides these security service assurances:

- **Confidentiality** – Information is not disclosed to unauthorized individuals, processes, or devices.
- **Data Integrity** – Unauthorized individuals, processes, or devices cannot alter information in a way not detectable by authorized individuals, processes, or devices.
- **Authentication** – Individuals, processes, or devices are who or what they claim to be.
- **Non-repudiation** – Individuals, processes, or devices involved in a communication or transaction cannot later claim the communication or transaction did not occur (works in conjunction with authentication).
- **Access Control** – Resources and services can only be accessed by authorized individuals and unauthorized individuals are denied access.

PKI Components

PKI is comprised of hardware/software products and policies/procedures, and supports the security framework required to conduct e-business. PKI consists of the following mechanisms:

- **Digital Certificates** – Electronic information about a subscriber, signed by a trusted certificate authority.
- **Digital Keys** – three sets of key pairs exist and each set consists of a public and private key:
  - Identify
  - Signature
  - Encryption
- **A Token** – the physical mechanism that holds and protects the keys. The token can be various media such as the Common Access Card (CAC) or a disk. The CAC is the primary token chosen by the DoD.